| Reply to Pre-bid Queries | | | | | |
|---|---|---|---|---|---|
| TENDER DOCUMENT NO. IGL/ET2/CP/CM17506 | | | | | |
| HIRING OF CLOUD BASED WEB APPLICATION FIREWALL (WAF) SERVICE FOR IGL | | | | | |
| | | | | | |
| **Sl No** | **RFP Clause** | **Description** | **Query** | **Revised Clause as per Query (Requested by Vendor)** | **IGL Response** |
| 1 | Technical BEC 7.1 (a) | | Allow Bidder or OEM for valid ISO certification | Allow Bidder or OEM for valid ISO certification | Tender condition prevails |
| 2 | 7.1 (B) | | Allow Start up for bidding | Allow Start up for bidding | Tender condition prevails |
| 3 | 7.3 | | Allow to show Work order by Bidder/OEM | Allow to show Work order by Bidder/OEM | Tender condition prevails |
| 4 | Bid Security 11.1 | | Exempt EMD for Start up | Exempt EMD for Start up | Tender condition prevails |
| 5 | Clause 8, page 51 | Penalty | Kindly Limit this upto 5% of order value | Kindly Limit this upto 5% of order value | Tender condition prevails |
| 6 | Clause 12/6, Page 53 | The Cloud service provider should have complied with ISO 27017(Information security for cloud service). | Our underling cloud infrastructure provider is compliant with this cert ISO 27017, Will AWS publically available Cert will comply for this? | Our underling cloud infrastructure provider is compliant with this cert ISO 27017, Will AWS publically available Cert will comply for this? | Clarification:<br>Bidder has to submit the required supporting documents signed with company seal/ digitally signed. |
| 7 | Sec: V, WAF Pt.no.6 ,Page 60 | The proposed solution must offer out of band programming for control plane along with data plane scripting for functions like content inspection and traffic management. The proposed WAF should be capable to trigger a script based on an event. | Please provide use case of this requirement. This looks more towords onsite/ on-premise solution feature. As this is RFP for cloud solution this should be excluded from requirement. Kindly remove this clause as its not relevant in case of WAF | Please provide use case of this requirement. This looks more towords onsite/ on-premise solution feature. As this is RFP for cloud solution this should be excluded from requirement. Kindly remove this clause as its not relevant in case of WAF | Tender condition prevails |
| 8 | Sec V, SOW, Page 64 | Response and Resolution Times | We hope this response time is regarding availability of the WAF solution, kindly confirm on this. | We hope this response time is regarding availability of the WAF solution, kindly confirm on this. | This is regarding resolution time of the issue/ticket rasied. |
| 9 | Clause 7.1, page 8 | The bidder must have a valid ISO 27001 certification | Kinldy relax this criteria to either Bidder/ OEM should have ISO27001 Certification | Kinldy relax this criteria to either Bidder/ OEM should have ISO27001 Certification | Tender condition prevails |
| 10 | Clause 7.2 C, page 9 | The working capital of the bidder should not be less than 6.42L in the preceding financial year | we would like to confirm that the preceding year will be 2021-2022 since for the last financial year we don't have audited financials yet | we would like to confirm that the preceding year will be 2021-2022 since for the last financial year we don't have audited financials yet | Preceding FY is 2021-22 |

Digitally signed by NISHA BHINGE
Date: 2023.05.19 15:00:19 IST

| | | | | | |
|---|---|---|---|---|---|
| 11 | clause 12.9, page 53 | The total bandwidth consumed for the solution is calculated on aggregate basis(200GB/Month per App) and for all application the total consumed bandwidth consumed would be at least 4000GB/Month(i.e. 200GB/Months x 20 Apps) for all the application. Billing model should be "Pay as go" model. | Where can we mention prices for additional data | Where can we mention prices for additional data | Tender condition prevails |
| 13 | Page 62 / Section V / Scope of Work / API Security | The solution should protect for those applications that allow users to upload files, the solution should enforce file upload restrictions based on file extension and file content. | Recommending change as:<br><br>The solution should protect for those applications that allow users to upload files, the solution should enforce file upload restrictions based on file extension and file content including AV scanning | | Tender condition prevails |
| 14 | Page 64 / Section V / Scope of Work / Technical Specifications - WAF | | Additional Recommendation: | Additional Recommendation: | Tender condition prevails |
| | | | The solution should have DLP features to identify and block sensitive | The solution should have DLP features to identify and block sensitive information | Tender condition prevails<br>Tender condition prevails |
| 15 | Page 64 / Section V / Scope of Work / Technical Specifications - WAF | | Additional Recommendation:<br><br>The centralized management solution should enforce Two Factor Authentication for user access. | Additional Recommendation:<br><br>The centralized management solution should enforce Two Factor Authentication for user access | Tender condition prevails |
| 16 | Page 64 / Section V / Scope of Work / Technical Specifications - WAF | | Additional Recommendation:<br><br>The proposed solution should provide Anti-defacement protection, parameters and hidden form fields obfuscation and protection against manipulation | Additional Recommendation:<br><br>The proposed solution should provide Anti-defacement protection, parameters and hidden form fields obfuscation and protection against manipulation | Tender condition prevails |
| 17 | Page 64 / Section V / Scope of Work / Technical Specifications - WAF | | Additional Recommendation:<br><br>The solution should have ability to create custom logging rules to allow / mask sensitive information from being logged by the Web Application Firewall | Additional Recommendation:<br><br>The solution should have ability to create custom logging rules to allow / mask sensitive information from being logged by the Web Application Firewall | Tender condition prevails |

| | | | | | |
|---|---|---|---|---|---|
| 18 | Page 64 / Section V / Scope of Work / Technical Specifications - WAF | | Additional Recommendation:<br><br>The solution should have deception capability to implant decoys (fake links and forms) in any application without any changes to application or client. | Additional Recommendation:<br><br>The solution should have deception capability to implant decoys (fake links and forms) in any application without any changes to application or client. | Tender condition prevails |
| 19 | Page 64 / Section V / Scope of Work / Technical Specifications - WAF | | Additional Recommendation:<br><br>The solution offered should be dedicated infrastructure for IGL and should be hosted within India on MeiTy empanneled CSPs | Additional Recommendation:<br><br>The solution offered should be dedicated infrastructure for IGL and should be hosted within India on MeiTy empanneled CSPs | Tender condition prevails |
| 20 | Web Application Firewall Under: Section V / Scope of Work / API Security, page 62 | The solution should protect for those applications that allow users to upload files, the solution should enforce file upload restrictions based on file extension and file content | Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br>Request you to please remove the given clause:<br>(The solution should protect for those applications that allow users to upload files, the solution should enforce file upload restrictions based on file extension and file content)<br><br>Ths clause should be read as-<br>The solution should protect for those applications that allow users to upload files, the solution should enforce file upload restrictions based on file extension and file content including AV scanning | Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br>Request you to please remove the given clause:<br>(The solution should protect for those applications that allow users to upload files, the solution should enforce file upload restrictions based on file extension and file content)<br><br>Ths clause should be read as-<br>The solution should protect for those applications that allow users to upload files, the solution should enforce file upload restrictions based on file extension and file content including AV scanning | Tender condition prevails |
| 21 | Web Application Firewall Under :Section V / Scope of Work / Technical Specifications - WAF, Page 64 | | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The solution should have DLP features to identify and block sensitive information such as credit card numbers, Aadhar Numbers, etc. | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The solution should have DLP features to identify and block sensitive information such as credit card numbers, Aadhar Numbers, etc. | Tender condition prevails |

| | | | | | |
|---|---|---|---|---|---|
| 22 | Web Application Firewall Under :Section V / Scope of Work / Technical Specifications - WAF, Page 64 | | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The solution should have DLP features to identify and block sensitive information such as credit card numbers, Aadhar Numbers, etc. | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The solution should have DLP features to identify and block sensitive information such as credit card numbers, Aadhar Numbers, etc. | Tender condition prevails |
| 23 | Web Application Firewall Under : Section V / Scope of Work / Technical Specifications - WAF, page 64 | | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The centralized management solution should enforce Two Factor Authentication for user access | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The centralized management solution should enforce Two Factor Authentication for user access | Tender condition prevails |
| 24 | Web Application Firewall Under : Section V / Scope of Work / Technical Specifications - WAF, page 64 | | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The proposed solution should provide Anti-defacement protection, parameters and hidden form fields obfuscation and protection against manipulation | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The proposed solution should provide Anti-defacement protection, parameters and hidden form fields obfuscation and protection against manipulation | Tender condition prevails |
| 25 | Web Application Firewall Under : Section V / Scope of Work / Technical Specifications - WAF, page 64 | | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The solution should have ability to create custom logging rules to allow / mask sensitive information from being logged by the Web Application Firewall | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The solution should have ability to create custom logging rules to allow / mask sensitive information from being logged by the Web Application Firewall | Tender condition prevails |

| | | | | | |
|---|---|---|---|---|---|
| 26 | Web Application Firewall<br>Under : Section V / Scope of Work / Technical Specifications - WAF, page 64 | | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The solution should have deception capability to implant decoys (fake links and forms) in any application without any changes to application or client. | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The solution should have deception capability to implant decoys (fake links and forms) in any application without any changes to application or client. | Tender condition prevails |
| 27 | Web Application Firewall<br>Under : Section V / Scope of Work / Technical Specifications - WAF, page 64 | | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The solution offered should be dedicated infrastructure for IGL and should be hosted within India on MeiTy empanneled CSPs | Dear Sir,<br>Please refer to Tender No IGL/ET2/CP/CM17506,Department of INDRAPRASTHA GAS LIMITED.<br><br>Request you to please add the given clause :<br>The solution offered should be dedicated infrastructure for IGL and should be hosted within India on MeiTy empanneled CSPs | Tender condition prevails |
| 28 | SECTION V, SCOPE OF WORK<br>Page 60 | Scans behind authenticated pages is part of the scope. Authentication details should be provided when the site is on-boarded. | We understand that the requirement is to protect the application whether authenticated or not authenticated. We Request to Clarify the same.<br><br>Suggested Clause :<br>Please clarify the understanding. | We understand that the requirement is to protect the application whether authenticated or not authenticated. We Request to Clarify the same.<br><br>Suggested Clause :<br>Please clarify the understanding. | Clarification:<br>If required authentication details shall be provided to sucessful cloud WAF provider after on boarded. |
| 29 | SECTION V, SCOPE OF WORK<br>Page 61<br>WAF<br>Sl. No 9 | The Proposed Solution should have capability to support minimum 5000 https Concurrent Connections scalable to 10000 https Concurrent Connections. | As per Industry Standard, Cloud WAF sizing are considered on the basis of bandwidth of the application and number of Applications to be protected. Hence request you to please amend the clause:<br><br>Suggested Clause :<br>The proposed Cloud Application Security Service should support 20 Applications and provide 100 Mbps HTTP/S traffic from day 1 | As per Industry Standard, Cloud WAF sizing are considered on the basis of bandwidth of the application and number of Applications to be protected. Hence request you to please amend the clause:<br><br>Suggested Clause :<br>The proposed Cloud Application Security Service should support 20 Applications and provide 100 Mbps HTTP/S traffic from day 1 | Clarification:<br>This is for the capability of cloud WAF. This capability is not required from day 1 but it should be there in future requirements. |

| | | | | | |
|---|---|---|---|---|---|
| 30 | SECTION V, SCOPE OF WORK<br>Page 61<br>WAF<br>Sl. No 17 | Proposed WAF Solution should have functionality to showcase how many URLs in the application have been completely learned & move them into Protection Mode automatically i.e. some URLs to be in learning mode & some URLs in the Protection Mode of the same Application. | After the learning period, policies needs to be generated automatically and it should be reviewed manually by the OEM Specialized ERT team before putting the application into the blocking mode. As putting the application into the blocking mode automatically after few days of learning may result into high number of False Positive & False Negative and can impact the user experience accessing the application.<br><br>And the application needs to be completely into the learning mode or completely into the Blocking Mode, as if some URI's are kept in learning mode means they will not block any malicious transaction, keeping your application vulnerable. Attacker can access one path of the application which was kept in learning and can compromise the entire application and it is highly recommended to keep all the URI/Paths of the application completely into the<br>learning or blocking. However you can put the application into the partial blocking mode by keeping few of the security parameters into the learning for fine-tuning of the application policies and few security parameter into blocking. Hence Request you to please amend the clause: | After the learning period, policies needs to be generated automatically and it should be reviewed manually by the OEM Specialized ERT team before putting the application into the blocking mode. As putting the application into the blocking mode automatically after few days of learning may result into high number of False Positive & False Negative and can impact the user experience accessing the application.<br><br>And the application needs to be completely into the learning mode or completely into the Blocking Mode, as if some URI's are kept in learning mode means they will not block any malicious transaction, keeping your application vulnerable. Attacker can access one path of the application which was kept in learning and can compromise the entire application and it is highly recommended to keep all the URI/Paths of the application completely into the<br>learning or blocking. However you can put the application into the partial blocking mode by keeping few of the security parameters into the learning for fine-tuning of the application policies and few security parameter into blocking. Hence Request you to please amend the clause:<br><br>Suggested Clause :<br>The Proposed Cloud WAF Solution should learns the patterns of legitimate user activities and automatically builds security | Clarification:<br><br>Machine learning and protection is a contnuous process, the solution should have functionality of machine learning process to detect and prevents the threats using machine learning technique that can learn the pattern of attack vectors and this can provide an extra layer of prtoection , bring down the false postive rates, malicious attack and leads to imporved threat detection rate. |

| | | | | | |
|---|---|---|---|---|---|
| 32 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 64<br>WAF Salient Feature<br>Sl. No 11 | The solution should provide protection against known vulnerabilities like OWASP Top 10 vulnerabilities, SANS Top 25 Vulnerabilities and WASC Web Security Attack classification. | The OWASP Top 10 is a standard awareness document and industry standard guidelines which are considered by developers for security assessment of any application. Solution might not follow other guideline but the solution should be capable to protect the application against OWSAP Top 10 attacks, hacking, vulnerabilities and beyond.<br><br>Suggested Clause :<br>The solution should provide protection against known vulnerabilities like OWASP Top 10 vulnerabilities and WASC Web Security Attack classification. | The OWASP Top 10 is a standard awareness document and industry standard guidelines which are considered by developers for security assessment of any application. Solution might not follow other guideline but the solution should be capable to protect the application against OWSAP Top 10 attacks, hacking, vulnerabilities and beyond.<br><br>Suggested Clause :<br>The solution should provide protection against known vulnerabilities like OWASP Top 10 vulnerabilities and WASC Web Security Attack classification. | Tender condition prevails |
| 33 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 64<br>WAF Salient Feature<br>Sl. No 15 | WAF should support 20,000 HTTP/HTTPS transactions per second | As per Industry Standard, Cloud WAF sizing are considered on the basis of bandwidth of the application and number of Applications to be protected. Hence request you to please amend the clause:<br><br>Suggested Clause :<br>The proposed Cloud Application Security Service should support 20 Applications and provide 100 Mbps HTTP/S traffic from day 1 (Committed at any given point of Time) and no restriction based on Data Transfer. | As per Industry Standard, Cloud WAF sizing are considered on the basis of bandwidth of the application and number of Applications to be protected. Hence request you to please amend the clause:<br><br>Suggested Clause :<br>The proposed Cloud Application Security Service should support 20 Applications and provide 100 Mbps HTTP/S traffic from day 1 (Committed at any given point of Time) and no restriction based on Data Transfer. | Clarification:<br>This is for the capability of cloud WAF. This capability is not required from day 1 but it should be there in future requirements. |

| | | | | | |
|---|---|---|---|---|---|
| 34 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 64<br>WAF Salient Feature<br>Sl. No 16 | On request integration of new applications, increase in data transfer and throughput should be provided at quoted rates | CDN based Vendor does the sizing on the basis of data transfer, which is not the required for Cloud WAF Service Provider.<br>As per Industry Standard, for Cloud WAF sizing are considered on the basis of bandwidth of the application and number of Applications to be protected. Hence request you to please amend the clause:<br><br>Suggested Clause :<br>The proposed Cloud Application Security Service should support 20 Applications and provide 100 Mbps HTTP/S traffic from day 1 (Committed at any given point of Time). Solution should be highly scalable on the number of applications and bandwidth and there should not be any restriction based on Data Transfer. | CDN based Vendor does the sizing on the basis of data transfer, which is not the required for Cloud WAF Service Provider. As per Industry Standard, for Cloud WAF sizing are considered on the basis of bandwidth of the application and number of Applications to be protected. Hence request you to please amend the clause:<br><br>Suggested Clause :<br>The proposed Cloud Application Security Service should support 20 Applications and provide 100 Mbps HTTP/S traffic from day 1 (Committed at any given point of Time). Solution should be highly scalable on the number of applications and bandwidth and there should not be any restriction based on Data Transfer. | Tender condition prevails |
| 35 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 64<br>WAF Salient Feature | New Clause Request | Cyber Security is very important aspect in the entire datacenter and application deployed.<br><br>Suggested Clause :<br>The proposed solution should support NSS Lab recommended, ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification. | Cyber Security is very important aspect in the entire datacenter and application deployed.<br><br>Suggested Clause :<br>The proposed solution should support NSS Lab recommended, ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification. | Tender condition prevails |
| 36 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 64<br>WAF Salient Feature | New Clause Request | Cloud WAF platform should have capability to Protect Application with Custom Ports. The proposed solution should have an ability to support HTTP/HTTPS traffic delivery and inspection using a non-standard ports range between 1024 and 65534 | Cloud WAF platform should have capability to Protect Application with Custom Ports. The proposed solution should have an ability to support HTTP/HTTPS traffic delivery and inspection using a non-standard ports range between 1024 and 65534 | Tender condition prevails |
| 37 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 64<br>WAF Salient Feature | New Clause Request | CONTINUOUSLY ADAPTIVE SECURITY POLICIES: The proposed Service must offer dynamic security policies which learn traffic baselines automatically adapt to each individual application and its unique pattern of user traffic. | CONTINUOUSLY ADAPTIVE SECURITY POLICIES: The proposed Service must offer dynamic security policies which learn traffic baselines automatically adapt to each individual application and its unique pattern of user traffic. | Tender condition prevails |

| | | | | | |
|---|---|---|---|---|---|
| 38 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 64<br>WAF Salient Feature | New Clause Request | FRICTIONLESS API DISCOVERY : Automated API discovery algorithm that continuously discovers APIs and their endpoints and adapts to existing API endpoints definitions. Based on the discovered API catalogs, a tailored security policy should be generated to protect these APIs.<br><br>a) Auto-policy generation tailored per API endpoint<br>b) Completely automated discovery, generating an accurate API schema and a tailored security policy<br>c) Eliminate human errors; no human intervention required to complete the API discovery process<br>d) Keeps documented APIs security protection up to date by automatically discovering API changes | FRICTIONLESS API DISCOVERY : Automated API discovery algorithm that continuously discovers APIs and their endpoints and adapts to existing API endpoints definitions. Based on the discovered API catalogs, a tailored security policy should be generated to protect these APIs.<br><br>a) Auto-policy generation tailored per API endpoint<br>b) Completely automated discovery, generating an accurate API schema and a tailored security policy<br>c) Eliminate human errors; no human intervention required to complete the API discovery process<br>d) Keeps documented APIs security protection up to date by automatically discovering API changes | Tender condition prevails |
| 39 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 66 | New Clause Request | INTENT-BASED DEEP BEHAVIORAL ANALYSIS (IDBA) : Identify the intent of bots with the highest precision through semi supervised machine learning models. | INTENT-BASED DEEP BEHAVIORAL ANALYSIS (IDBA) : Identify the intent of bots with the highest precision through semi supervised machine learning models. | Tender condition prevails |
| 40 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 66 | New Clause Request | Detect and identify bots using a multi-layered approach options for bot mitigation which includes block, feed fake data, CAPTCHA, throttle, drop, session terminate, redirect loop, log only and custom actions. | Detect and identify bots using a multi-layered approach options for bot mitigation which includes block, feed fake data, CAPTCHA, throttle, drop, session terminate, redirect loop, log only and custom actions. | Tender condition prevails |
| 41 | SECTION V, Technical Specifications - Web Application Firewall (WAF) | New Clause Request | Detect and block sophisticated humanlike bots in real time with no impact on the technology stack. | Detect and block sophisticated humanlike bots in real time with no impact on the technology stack. | Tender condition prevails |
| 42 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 66 | New Clause Request | Should support Crypto Mitigation algorithms that provides an option to enable genuine website visitors to enjoy a frictionless, CAPTCHA-free user experience. | Should support Crypto Mitigation algorithms that provides an option to enable genuine website visitors to enjoy a frictionless, CAPTCHA-free user experience. | Tender condition prevails |
| 43 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 66<br>Anti-Bot Detection | New Clause Request | FLEXIBLE INTEGRATION OPTIONS : Nonintrusive deployment using SDK, web server or content delivery network (CDN) plug-ins, JavaScript (JS) tag or as a reverse proxy — no impact on the technology | FLEXIBLE INTEGRATION OPTIONS : Nonintrusive deployment using SDK, web server or content delivery network (CDN) plug-ins, JavaScript (JS) tag or as a reverse proxy — no impact on the technology stack. | Tender condition prevails |

| | | | | | |
|---|---|---|---|---|---|
| 44 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 66 | New Clause Request | OEM should provide support for fine-tuning, policy review, monitoring, alerting, and troubleshooting with unlimited No of Rules/Policies creation without any additional cost. | OEM should provide support for fine-tuning, policy review, monitoring, alerting, and troubleshooting with unlimited No of Rules/Policies creation without any additional cost. | Tender condition prevails |
| 45 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 66 | New Clause Request | **There should be Periodic security-status reporting** | **There should be Periodic security-status reporting** | Tender condition prevails |
| 46 | SECTION V, Technical Specifications - Web Application Firewall (WAF)<br>Page 66 | New Clause Request | **There should be provision for Post-attack forensics and recommendations** | **There should be provision for Post-attack forensics and recommendations** | Tender condition prevails |
| 48 | Point no. 38, Technical Specifications - Web Application Firewall (WAF)-Anti-Bot Detection<br>Page no 66 | Mobile Application Identification: For mobile clients that cannot execute Java script or CAPTCHA, Solution should verify the request is legitimate by verifying the JTW-token a mobile application carries when it access a web server | Mobile Application Identification: For mobile clients that cannot execute Java script or CAPTCHA, Solution should verify the request is legitimate by verifying the JTW-token a mobile application carries when it access a web server | **Please remove this OEM specific clause**<br>We would like to request the honorable tendering committee to amend this clause for wider participation and to get the best technocommercial solution available in the market. | Clarification:<br>Kindly ignore OEM sepecific terminology, if any. The solution proposed should meet the IGL requirements. |
| 49 | 7.0 BIDDER EVALUATION CRITERIA (BEC)<br>Page no 9 | The Bidder should have experience of successfully executed work order of providing of cloud based web application firewall (WAF) of at least Rs. 16.05 Lacs (incl. GST) for preceding last 7 years from date of floating of tender. | The Bidder should have experience of successfully executed work order of providing of cloud based web application firewall (WAF) of at least Rs. 16.05 Lacs (incl. GST) for preceding last 7 years from date of floating of tender. | We have NDA signed with most of our Customers and will not be able to submit PO and completion certificate.<br>**Request to allow submisison of CA certificate against PO and completion certificate or**<br>**Please allow internal orders (PO and Completion) within company implemented/executed for different department to be considered.** | Tender condition prevails |

Digitally signed by NISHA BHINGE
Date: 2023.05.19 15:00:19 IST